IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT : Tomoyuki Asano et al.
APPLICATION No. : 09/807,824 Group Art Unit : 2131
FILING DATE : April 18, 2001 Examiner : Jackson, J.
TITLE : Information Transmission System and Method, Drive Device and Access Method, Information Recording Medium, Device and Method for Producing Recording Medium

Hon. Commissioner of Patents and Trademarks,
Washington, D.C. 20231

SIR:

CERTIFIED TRANSLATION

I, Takashi Narita, am an official translator of the Japanese language into the English language and I hereby certify that the attached comprises an accurate translation into English of Japanese Application No. 11-234371, filed on August 20, 1999.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

December 6, 2006

Date

Takashi Narita

Takashi Narita

[Document Name] Patent Application

[Reference Number] 9900417005

[Filing Date] August 20, 1999

[To] Hon.Commissioner, Patent Office

[IPC] G11B 7/00

[Inventor]

[Address] c/o Sony Corporation

7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo, Japan

[Name] Tomoyuki Asano

[Inventor]

[Address] c/o Sony Corporation

7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo, Japan

[Name] Yoshitomo Osawa

[Patent Applicant]

[Identification Number] 000002185

[Name] Sony Corporation

[Representative] Nobuyuki Idei

[Patent Attorney]

[Identification Number] 100067736

[Patent Attorney]

[Name] Akira Koike

[Patent Attorney]

[Identification Number] 100086335

[Patent Attorney]

[Name] Eiichi Tamura

[Patent Attorney]

[Identification Number] 100096677

[Patent Attorney]

[Name] Seiji Iga

[Indication of Charge]

[Number of Prepaid Ledger] 019530

[Amount] 21,000 yen

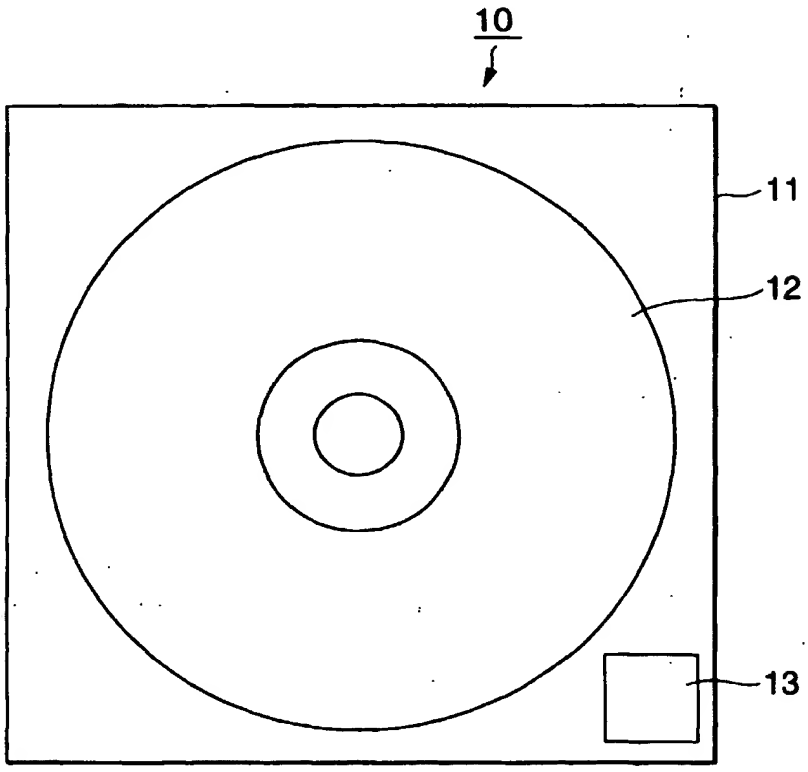
[List of Document]

| | | |
|---|---|---|
| [Document] | Specification | 1 |
| [Document] | Drawing | 1 |
| [Document] | Summary | 1 |
| [General Power of Attorney Number] | | 9707387 |

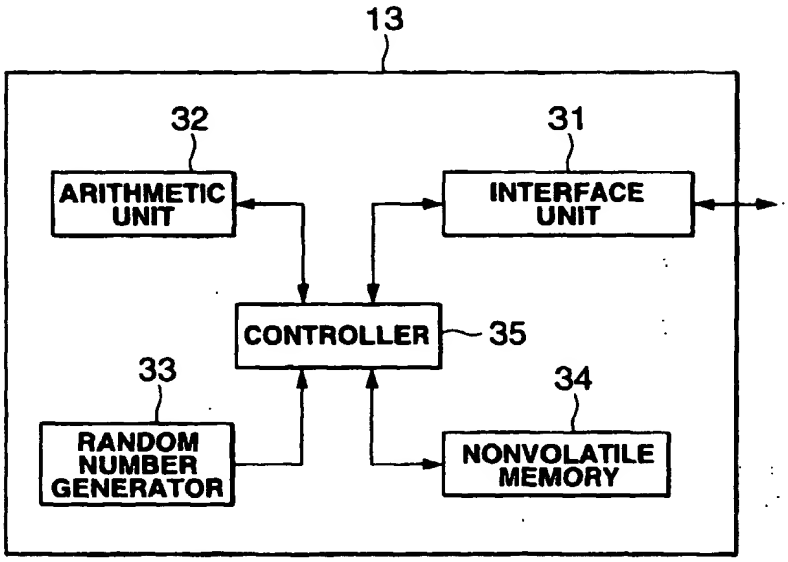
[Need of Proof] Yes

[DOCUMENT NAME] DRAWING

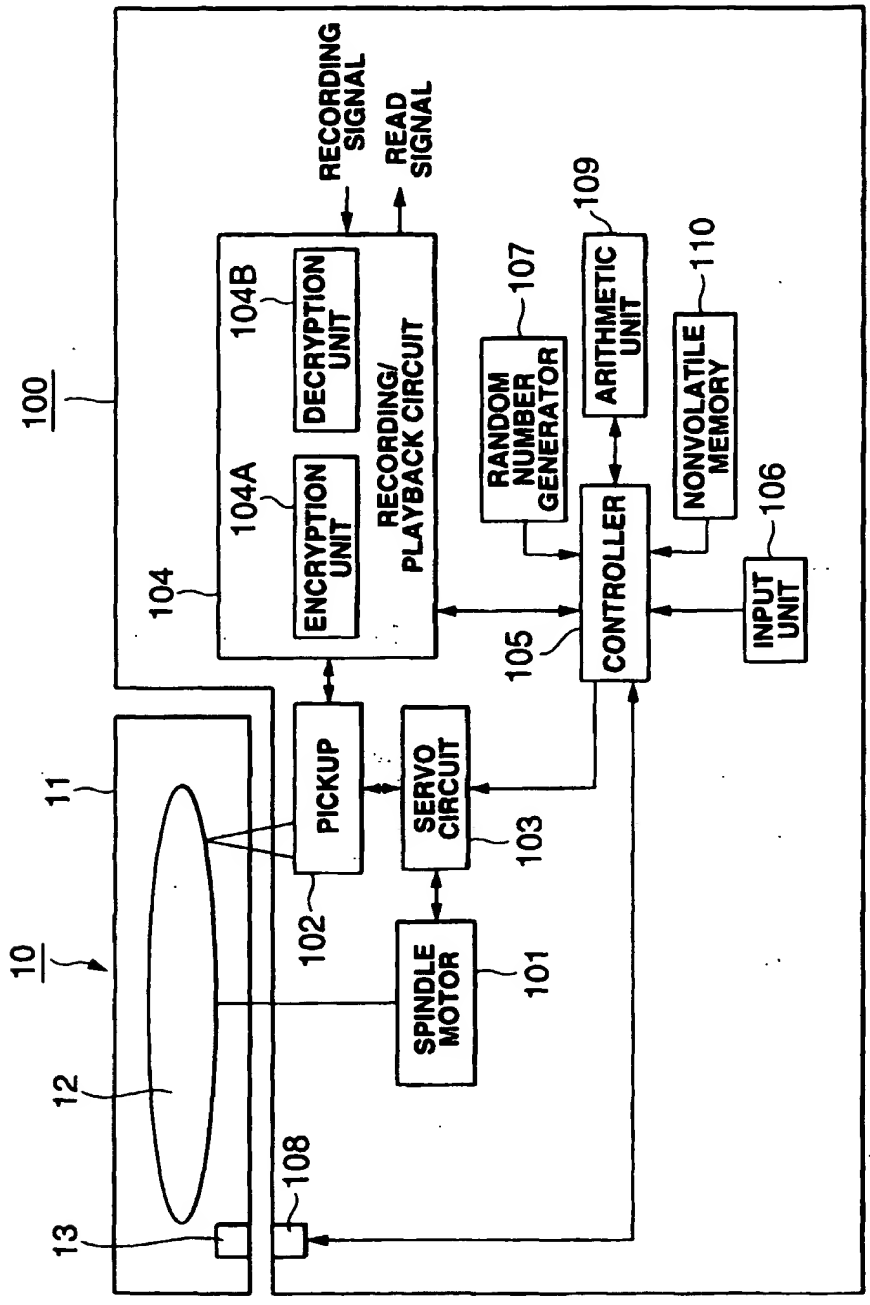
[FIG. 1]



[FIG. 2]


13
32
ARITHMETIC UNIT
31
INTERFACE UNIT
CONTROLLER
35
33
RANDOM NUMBER GENERATOR
34
NONVOLATILE MEMORY

[FIG. 3]

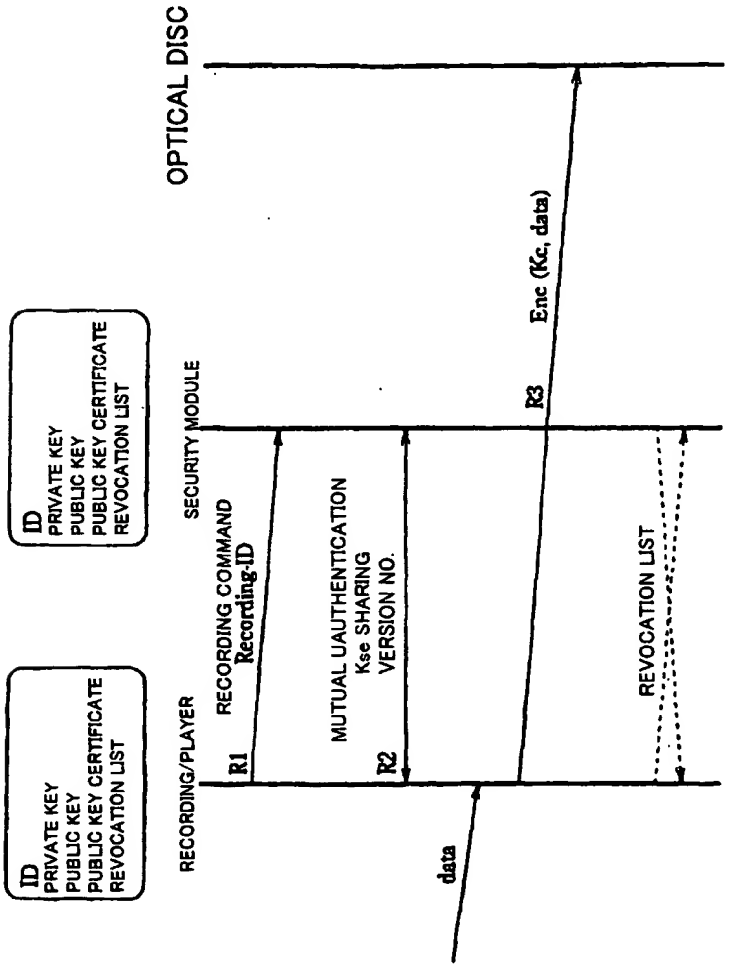

100
10
11
12
13
108
PICKUP
102
SERVO CIRCUIT
103
SPINDLE MOTOR
101
104
104A
ENCRYPTION UNIT
104B
DECRYPTION UNIT
RECORDING/ PLAYBACK CIRCUIT
RECORDING SIGNAL
READ SIGNAL
105
CONTROLLER
RANDOM NUMBER GENERATOR
107
ARITHMETIC UNIT
109
NONVOLATILE MEMORY
110
INPUT UNIT
106

[FIG. 4]

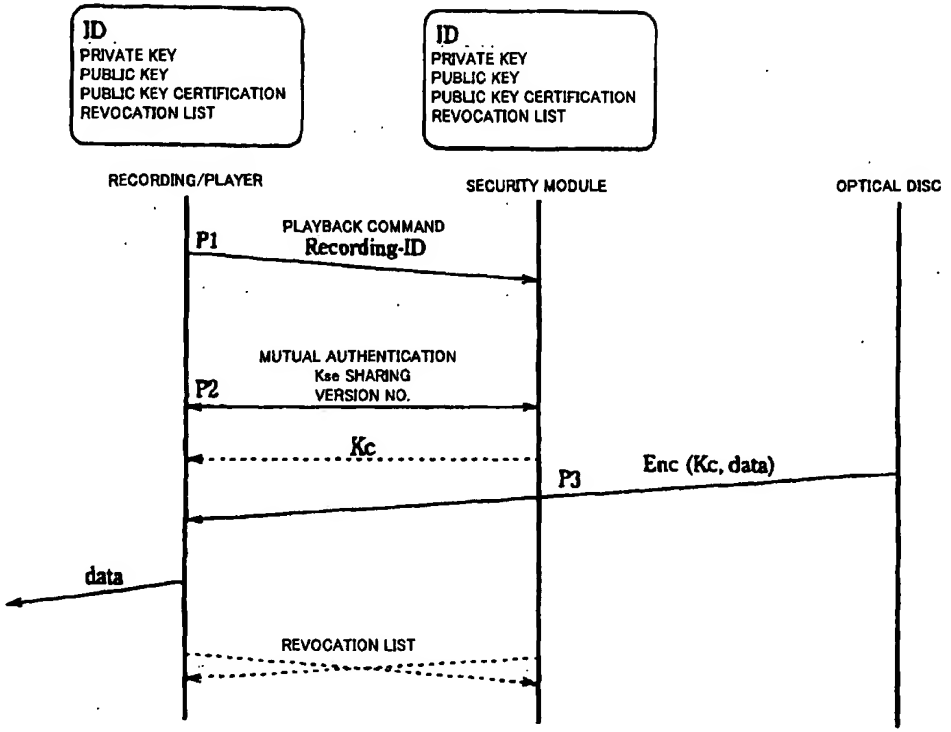
REVOCATION LIST

| VERSION NO. |
| --- |
| ID OF UNIT OR MEDIUM TO BE REVOKED |
| . . . . . |
| |
| DIGITAL SIGNATURE BY TC |

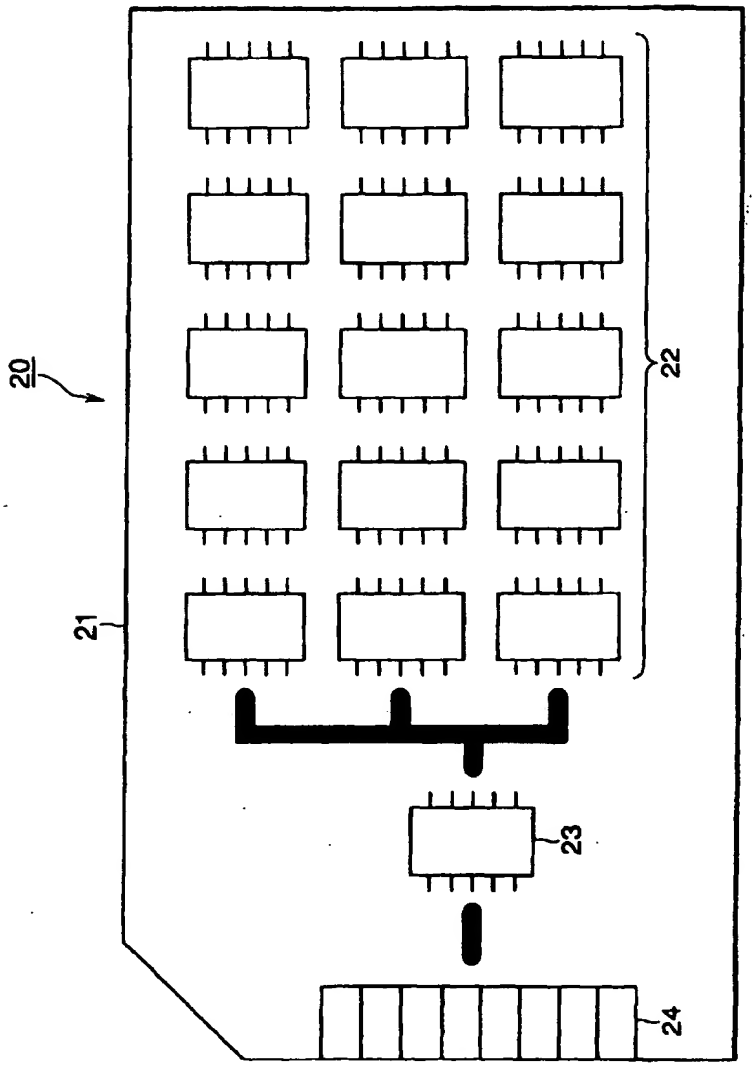
[FIG. 5]


ID
PRIVATE KEY
PUBLIC KEY
PUBLIC KEY CERTIFICATE
REVOCATION LIST
ID
PRIVATE KEY
PUBLIC KEY
PUBLIC KEY CERTIFICATE
REVOCATION LIST
OPTICAL DISC
RECORDING/PLAYER
SECURITY MODULE
RECORDING COMMAND
Recording-ID
R1
MUTUAL UAUTHENTICATION
Kse SHARING
VERSION NO.
R2
R3
Enc (Kc, data)
REVOCATION LIST
data

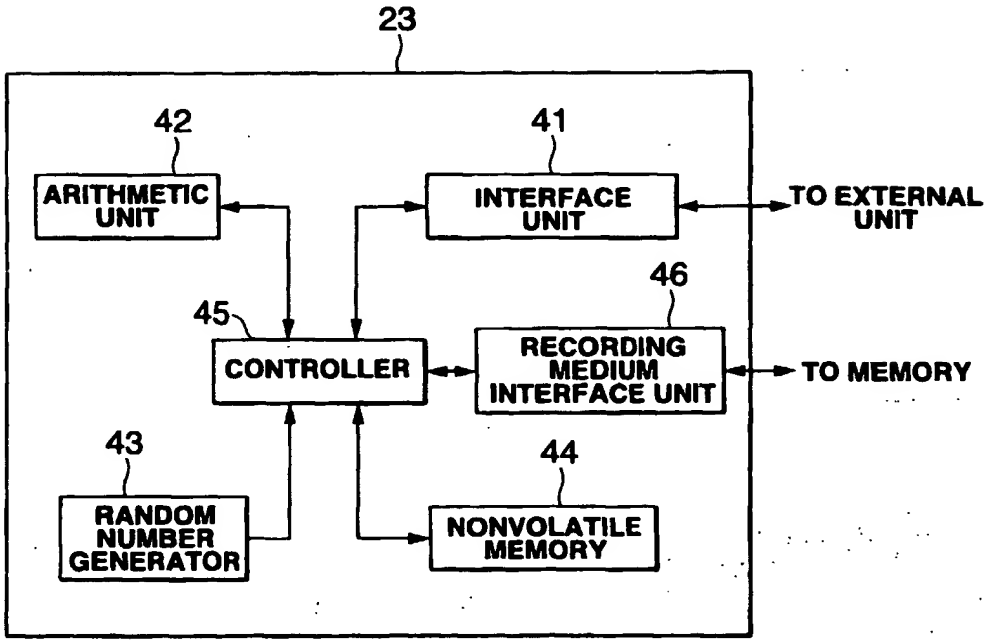
[FIG. 6]


ID
PRIVATE KEY
PUBLIC KEY
PUBLIC KEY CERTIFICATION
REVOCATION LIST
ID
PRIVATE KEY
PUBLIC KEY
PUBLIC KEY CERTIFICATION
REVOCATION LIST
RECORDING/PLAYER
SECURITY MODULE
OPTICAL DISC
P1
PLAYBACK COMMAND
Recording-ID
MUTUAL AUTHENTICATION
Kse SHARING
VERSION NO.
P2
Kc
Enc (Kc, data)
P3
data
REVOCATION LIST

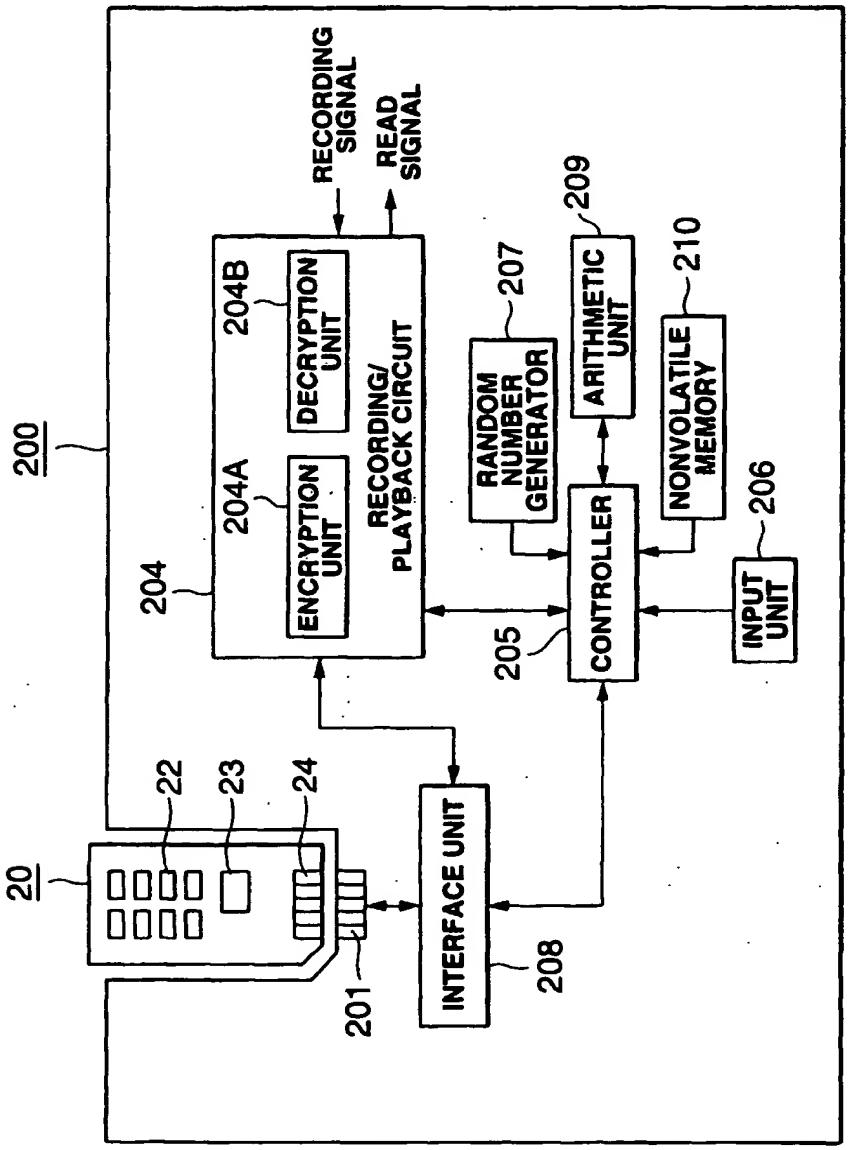
[FIG. 7]



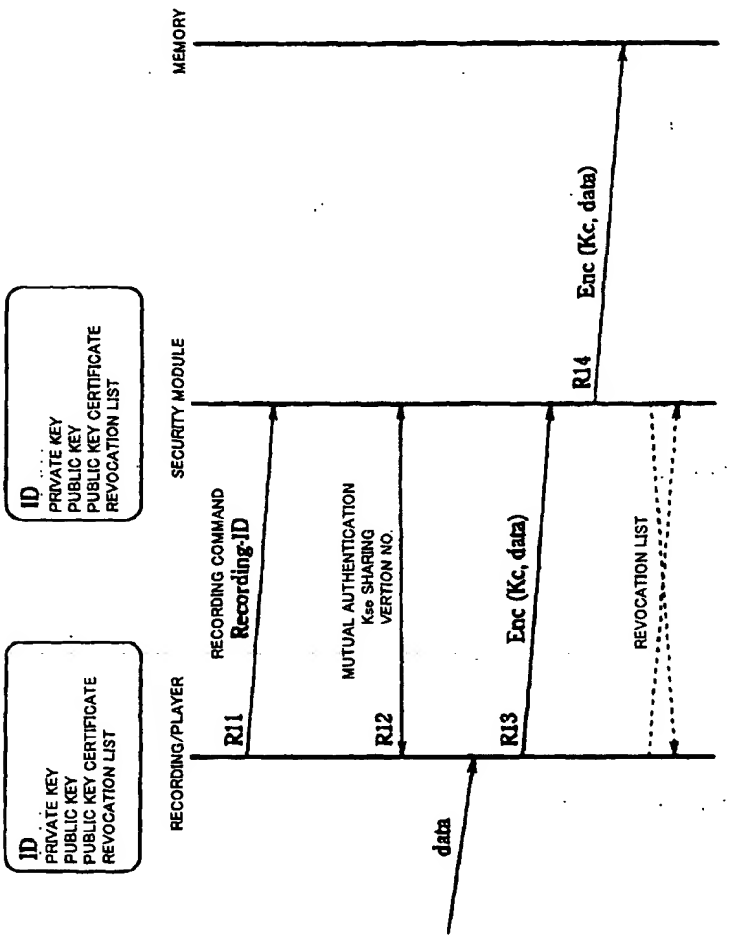
[FIG. 8]


23
42
ARITHMETIC UNIT
41
INTERFACE UNIT
TO EXTERNAL UNIT
46
45
CONTROLLER
RECORDING MEDIUM INTERFACE UNIT
TO MEMORY
43
RANDOM NUMBER GENERATOR
44
NONVOLATILE MEMORY

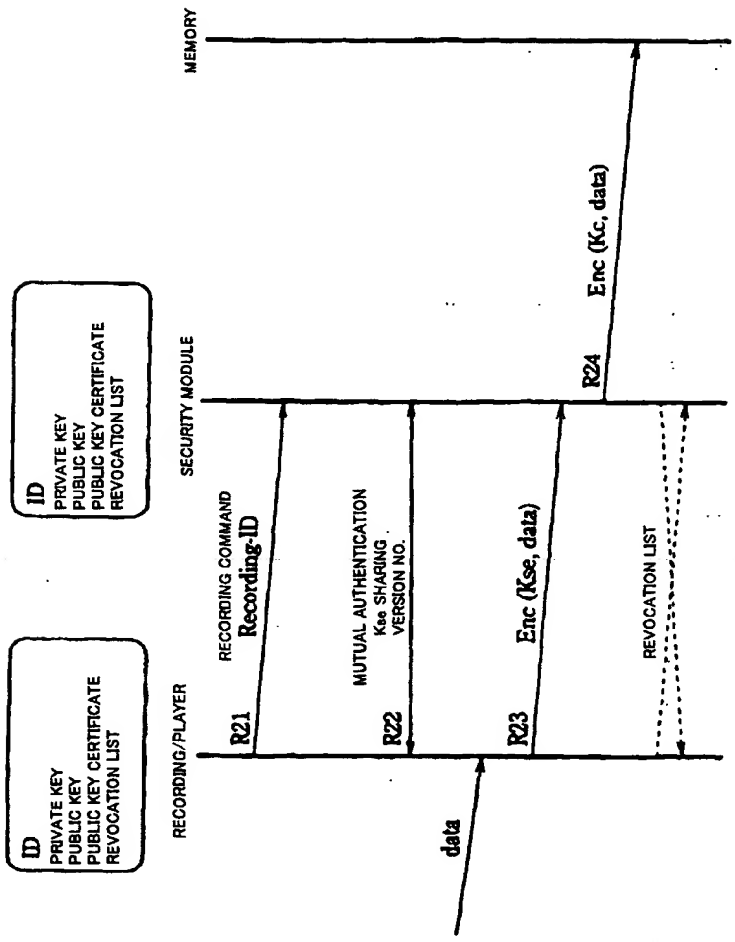
[FIG. 9]


200
20
22
23
24
201
INTERFACE UNIT
208
204
204A
ENCRYPTION UNIT
204B
DECRYPTION UNIT
RECORDING/ PLAYBACK CIRCUIT
RECORDING SIGNAL
READ SIGNAL
205
CONTROLLER
RANDOM NUMBER GENERATOR
207
ARITHMETIC UNIT
209
NONVOLATILE MEMORY
210
INPUT UNIT
206

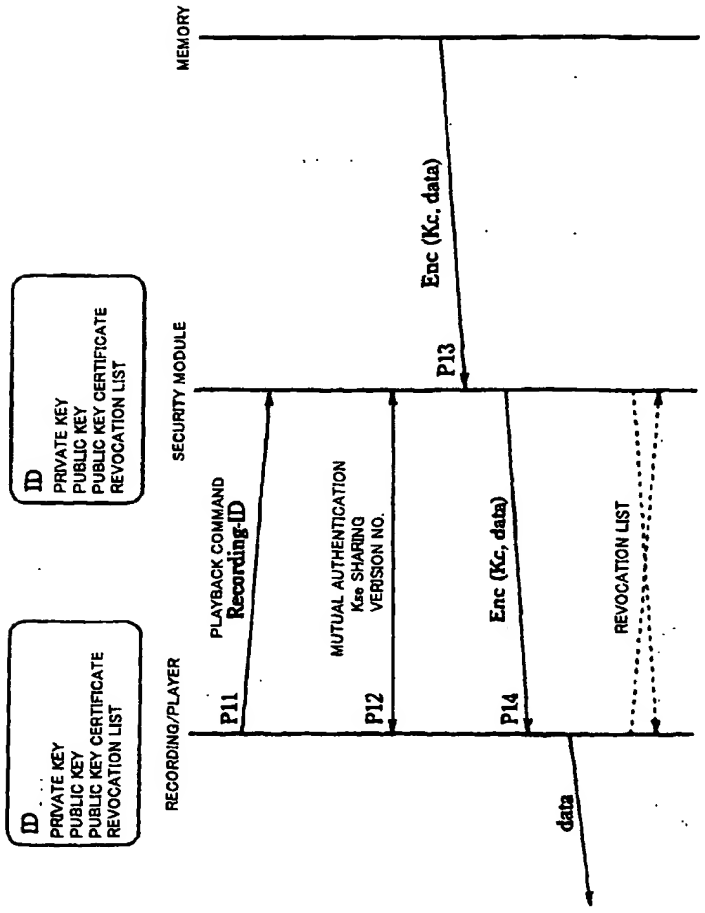
[FIG. 10]


ID
PRIVATE KEY
PUBLIC KEY
PUBLIC KEY CERTIFICATE
REVOCATION LIST
ID
PRIVATE KEY
PUBLIC KEY
PUBLIC KEY CERTIFICATE
REVOCATION LIST
RECORDING/PLAYER
SECURITY MODULE
MEMORY
RECORDING COMMAND
Recording-ID
R11
MUTUAL AUTHENTICATION
Kse SHARING
VERTION NO.
R12
R13
Enc (Kc, data)
R14
Enc (Kc, data)
REVOCATION LIST
data

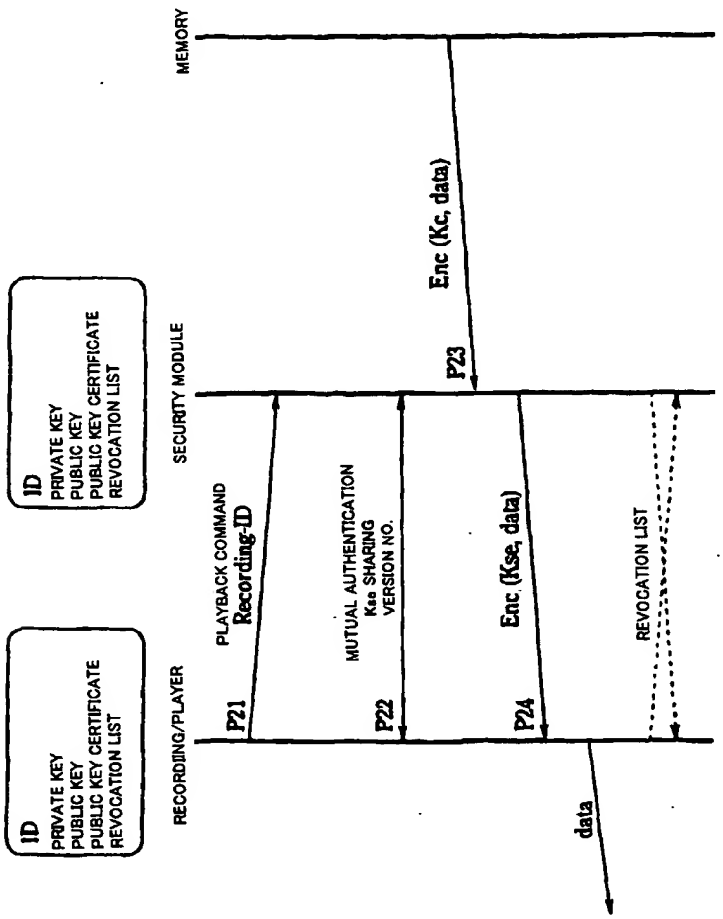
[FIG. 11]


ID
PRIVATE KEY
PUBLIC KEY
PUBLIC KEY CERTIFICATE
REVOCATION LIST
ID
PRIVATE KEY
PUBLIC KEY
PUBLIC KEY CERTIFICATE
REVOCATION LIST
RECORDING/PLAYER
SECURITY MODULE
MEMORY
RECORDING COMMAND
Recording-ID
R21
MUTUAL AUTHENTICATION
Kse SHARING
VERSION NO.
R22
Enc (Kse, data)
R23
REVOCATION LIST
Enc (Kc, data)
R24
data

[FIG. 12]


ID
PRIVATE KEY
PUBLIC KEY
PUBLIC KEY CERTIFICATE
REVOCATION LIST
ID
PRIVATE KEY
PUBLIC KEY
PUBLIC KEY CERTIFICATE
REVOCATION LIST
RECORDING/PLAYER
SECURITY MODULE
MEMORY
P11
PLAYBACK COMMAND
Recording-ID
P12
MUTUAL AUTHENTICATION
Kse SHARING
VERISION NO.
P13
Enc (Kc, data)
P14
Enc (Kc, data)
REVOCATION LIST
data

[FIG. 13]


ID
PRIVATE KEY
PUBLIC KEY
PUBLIC KEY CERTIFICATE
REVOCATION LIST
ID
PRIVATE KEY
PUBLIC KEY
PUBLIC KEY CERTIFICATE
REVOCATION LIST
RECORDING/PLAYER
SECURITY MODULE
MEMORY
PLAYBACK COMMAND
Recording-ID
P21
MUTUAL AUTHENTICATION
Kse SHARING
VERSION NO.
P22
Enc (Kc, data)
P23
Enc (Kse, data)
P24
REVOCATION LIST
data

[Name of Document] ABSTRACT

[Summary]

[Task]

To enable to prevent copyrighted data such as movie, music, etc. from being copied illegally (against the wish of the copyrighter of the data).

[Means for Solution]

A security module 13 is provided in an optical disc medium 10, data to be written to the optical disc is encrypted with an content key different from one data to another, and the content key is safely stored in the security module 13. Also, the security module 13 makes a mutual authentication using the public-key encryption technology with a recording/playback device to check that the counterpart is an authorized and licensed unit, and then gives the content key to the counterpart, thereby preventing data from being leaked to any illegal device.

[Selected Drawing] FIG. 1

[Name of Document] SPECIFICATION

[Title of the Invention]

Data Recording/Playback System, Data Recording/Playback Apparatus and Method, and Data Recording Medium

[Claims]

[Claim 1]

A data recording/playback system comprising:

a data recording medium including a security module; and

a data recording/playback device for recording data encrypted with a content key controlled by the security module on the recording medium or playing back the data encrypted with the content key controlled by the security module from the recording medium,

wherein the data recording/playback device and the security module execute a mutual authentication protocol using the public-key encryption technology at the time of recording or playing back data.

[Claim 2]

The system as set forth in Claim 1, wherein the data recording/playback device and the security module respectively confirm at the time of executing the mutual authentication protocol that their counterpart's identification data (ID) is not placed in a revocation list.

[Claim 3]

The system as set forth in Claim 1, wherein, at the time of executing the mutual authentication protocol, the data recording/playback device and the security module teach the version numbers of their own revocation lists to each other, and one of them whichever has a newer revocation list sends the list to the other while the other having an older revocation list replaces its list with the received new list.

[Claim 4]

The system as set forth in Claim 1, wherein at the time of recording or playing back data, the data recording/playback device and security module execute a key sharing protocol using the public-key encryption technology, encrypt a data encrypting content key with a shared key thus obtained, and send the encrypted content key from one of them to the other.

[Claim 5]

The system as set forth in Claim 1, wherein at the time of recording or playing back data, the data recording/playback device and security module execute a key sharing protocol using the public-key encryption technology, encrypt data with a shared key thus obtained, and send the encrypted data from one of them to the other.

[Claim 6]

The system as set forth in Claim 1, wherein accesses to the data recording medium for storing data by writing and reading are performed via the security module.

[Claim 7]

The system as set forth in Claim 6, wherein, at the time of recording data, the

data recording/playback device and security module execute a key sharing protocol using the public-key encryption technology; the data recording/playback device encrypts data with a shared key and sends the encrypted data to the security module; and the security module decrypts the encrypted data with the shared key to obtain unencrypted data, re-encrypts the decrypted data with a content key, and stores the data in the data recording medium.

[Claim 8]

The system as set forth in Claim 6, wherein, at the time of playing back data, the security module reads out data encrypted and stored in the data recording medium and decrypts the data with the content key to obtain unencrypted data, and the security module encrypts the data with the shared key shared as a result of the key sharing protocol executed by the data recording/playback device and the security module and sends the data to the data recording/playback device.

[Claim 9]

A data recording medium comprising a security module for executing a mutual authentication protocol using a public-key encryption technology with a data recording/playback device at the time of recording and playing back data.

[Claim 10]

The recording medium as set forth in Claim 9, wherein the security module confirms at the time of executing the mutual authentication protocol that identification data (ID) of the data recording/playback device is not placed in a revocation list.

[Claim 11]

The recording medium as set forth in Claim 9, wherein, at the time of executing the mutual authentication protocol, the security module sends the version number of its own revocation list to the data recording/playback device, receives the version number of a revocation list sent by the data recording/playback device to compare its own number with the counterpart's number, sends the revocation list to the counterpart when its own revocation list is the newer, and replaces its own revocation list with the revocation list sent by the counterpart when the counterpart's revocation list is the newer.

[Claim 12]

The recording medium as set forth in Claim 9, which stores data encrypted with a content key controlled by the security module.

[Claim 13]

The recording medium as set forth in Claim 9, wherein at the time of recording and playing back data, the security module executes a key sharing protocol using the public-key encryption technology with the data recording/playback device, sends or receives a data encrypting content key to or from the encrypted data using the shared key.

[Claim 14]

The recording medium as set forth in Claim 9, wherein data writing and reading are performed via the security module.

[Claim 15]

The recording medium as set forth in Claim 14, wherein, at the time of recording data, the security module executes a key sharing protocol using the public-key encryption technology with the data recording/playback device, decrypts data received with the shared key, and re-encrypts the data with another key.

[Claim 16]

The recording medium as set forth in Claim 14, wherein, at the time of playing back data, the security module reads out data from the data recording medium and decrypts the data with the content key, executes the key sharing protocol using the public-key encryption technology with the data recording/playback device, encrypts data with the shared key, and sends the data to the data recording/playback device.

[Claim 17]

A data recording/playback apparatus comprising a control means for executing a mutual authentication protocol using a public-key encryption technology with a security module of a data recording medium at the time of recording and playing back data.

[Claim 18]

The recording/playback apparatus as set forth in Claim 17, wherein the control means confirms at the time of executing the mutual authentication protocol that identification data (ID) of the security module is not placed in a revocation list.

[Claim 19]

The recording/playback apparatus as set forth in Claim 17, wherein, at the time of executing the mutual authentication protocol, the control means sends the version number of its own revocation list to the security module, receives the version number of a revocation list sent by the security module to compare its own number with the counterpart's number, sends the revocation list to the counterpart when its own revocation list is the newer, and replaces its own revocation list with the revocation list sent by the counterpart when the counterpart's revocation list is the newer.

[Claim 20]

The recording/playback apparatus as set forth in Claim 17, which at the time of recording and playing back data, executes a key sharing protocol using the public-key encryption technology with the security module, and sends or receives a data encrypting content key to or from the security module.

[Claim 21]

The recording/playback apparatus as set forth in Claim 17, which at the time of recording data, executes a key sharing protocol using the public-key encryption technology with the security module, encrypts data with a shared key, and stores the data in the information recording medium.

[Claim 22]

The recording/playback apparatus as set forth in Claim 17, which at the time of recording data, executes a key sharing protocol using the public-key encryption technology with the security module, encrypts data with a shared key, and sends the

data to the security module.

[Claim 23]

The recording/playback apparatus as set forth in Claim 17, which, at the time of recording data, the control means executes a key sharing protocol using the public-key encryption technology with the security module, encrypts a data encrypting content key with a shared key, sends the key to the security module or receives a content key encrypted using the shared key from the security module, re-encrypts the data with the content key, and sends the data to the security module.

[Claim 24]

The recording/playback apparatus as set forth in Claim 17, wherein, at the time of playing back data, the control means executes a key sharing protocol using the public-key encryption technology with the security module, and decrypts data received from the security module using a shared key.

[Claim 25]

The recording/playback apparatus as set forth in Claim 17, which, at the time of playing back data, the control means executes a key sharing protocol using the public-key encryption technology with the security module, encrypts a data encrypting content key with a shared key, sends the key to the security module or receives a content key encrypted using the shared key from the security module, and decrypts the data received from the security module using the content key.

[Claim 26]

A data recording/playback method for recording or playing back data on or from a data recording medium by a data recording/playback device, comprising the step wherein:

a security module included in the data recording medium and the data recording/playback device execute a mutual authentication protocol using the public-key encryption technology.

[Claim 27]

The method as set forth in Claim 26, further comprising the step wherein:

the data recording/playback device and the security module respectively confirm at the time of executing the mutual authentication protocol that their counterpart's identification data (ID) is not placed in a revocation list.

[Claim 28]

The method as set forth in Claim 26, further comprising the steps, at the time of executing the mutual authentication protocol, wherein:

the data recording/playback device and the security module teach the version numbers of their own revocation lists to each other;

one of them whichever has a newer revocation list sends the list to the other; and

the other having an older revocation list replaces its list with the received new list.

[Claim 29]

The method as set forth in Claim 26, further comprising the steps, at the time

of recording or playing back data, wherein:

the data recording/playback device and security module execute a key sharing protocol using the public-key encryption technology; and

one of them encrypts a data encrypting content key with a shared key thus obtained, and sends the encrypted content key to the other.

[Claim 30]

The method as set forth in Claim 26, further comprising the steps, at the time of recording or playing back data, wherein:

the data recording/playback device and security module execute a key sharing protocol using the public-key encryption technology; and

one of them encrypts data with a shared key thus obtained, and sends the encrypted data to the other.

[Claim 31]

The method as set forth in Claim 26, further comprising the steps, at the time of recording data, wherein:

the data recording/playback device and security module execute a key sharing protocol using the public-key encryption technology;

the data recording/playback device encrypts data with a shared key and sends the encrypted data to the security module;

the security module decrypts the received data with the shared key;

the security module re-encrypts the decrypted data with a key; and

the security module stores the encrypted data in the data recording medium.

[Claim 32]

The method as set forth in Claim 26, further comprising the steps, at the time of playing back data, wherein:

the data recording/playback device and security module execute a key sharing protocol using the public-key encryption technology to share a key;

the security module reads out data from the data recording medium and decrypts the data with a key;

the security module encrypts the decrypted data with the shared key; and

the security module sends the encrypted data to the data recording/playback device.

[Claim 33]

A data recording medium comprising:

a security module having an interface function for interfacing with an external unit, a random number generating function, a data storing function, and a calculating function to provide a necessary calculation for mutual authentication protocol using the public-key encryption technology.

[Claim 34]

The data recording medium as set forth in Claim 33, wherein the security module further includes an interface function to access the data recording medium proper.

[Detailed Description of the Invention]

[0001]

[Technical Field of the Invention]

The present invention relates to a data recording/playback system, data recording/playback device and method, and data recording medium, which can safely transfer data.

[0002]

[Prior Art]

Recently, the recorder and recording medium, which can digitally record data, have been popular. Since video data and music data can be recorded to and played back from the recorder and recording medium without quality degradation, such data can be copied over and over again. Since such a digitally copied data keeps the very quality that the original data has, it will sell in the market. Because of this fact, however, the copyrighter of the video data or music data is afraid that his or her data will be copied many times and put on the market. In this circumstance, the recorder and recording medium are required to incorporate a feature of preventing copyrighted data from being illegally copied as above.

[0003]

For the copyright protection, a method called "Serial Copy Management System (SCMS)" is applied for the mini-disc (MD) (traded mark). In this system, SCMS data is transmitted along with music data. It indicates that the music data is one among

"copy free", "copy once allowed" or "copy prohibited". When a mini-disc (will be referred to as "MD" hereinafter) recorder receives music data from a digital interface, it will detect the SCMS data having been transmitted along with the music data. If the SCMS data is "copy prohibited", the MD recorder will not record the music data to the MD therein. If the SCMS data is "copy once allowed", the MD recorder will change the SCMS data to "copy prohibited" and record the SCMS data along with the received music data to the MD. If the SCMS data is "copy free", the MD recorder will record to the MD the SCMS data as it is along with the received music data.

[0004]

Using the SCMS data as in the above, the MD system prevents copyrighted data from illegally being copied.

[0005]

For prevention of copyrighted data from illegally being copied, another method is also available. It is called "content scramble system" and applied for the digital versatile disc (DVD) (trade mark) . In this system, all copyrighted data in a disc are encrypted and only a licensed recorder is given an content key to decrypt the encrypted data for acquisition of meaningful data. For getting licensed, the recorder is designed to conform an operation prescription against illegal copying etc. Thus the DVD system prevents copyrighted data from illegally being copied.

[0006]

[Problems to be Solved by the Invention]

In the method applied for the MD system, however, there may possibly be produced illegally a recorder which is not in conformity to the operation prescription that when the SCMS data is "copy once allowed", it should be changed to "copy prohibited" and recorded along with received data.

[0007]

The method adopted in the DVD system is effective on a read-only memory (ROM) medium, but not on a random-access memory (RAM) medium to which the user can record data. That is, even if the user cannot decrypt data in a RAM medium, he or she can illegally copy all data in the RAM medium in consideration to a new RAM medium which can be played in a licensed (legal) recorder.

[0008]

Thus, the Applicant of the present invention proposed a technique for prevention of illegal copying. This technique will briefly be described in the following. Namely, data intended for identification of individual recording media (will be referred to as "medium identification data" hereinafter) is recorded in each recording medium to allow only a licensed recorder to access the medium identification data as disclosed in the Applicant's Japanese Patent Application No. 10-25310 (Japanese Published Unexamined Patent Application No. 11-224461, issued on August 17, 1999). More specifically, data in a recording medium is encrypted using both a medium identification data and a key based on a secret acquired through licensing such that the data will be meaningless even if any unlicensed recorder can read it. Further, with this

technique, when a license is granted to a recorder , the operation of the recorder is prescribed not to make any illegally copying. Thus, with the above technique, the unlicensed recorder cannot access the data and the medium identification data for each medium takes a unique value, so that even if the unlicensed recorder copies all accessible data to a new medium for example, a licensed recorder will not be able to correctly read the data from the new medium.

[0009]

With the above conventional technique, however, to assure that a recording medium to which data has been recorded by a recorder can be read by another recorder, an content key for encryption of data in the recording medium is to be generated based on a common secret key (maser key) for the entire system. That is, if the master key is exposed through an attack to a recorder, all data recorded by any recorder included in the system will possibly be decrypted and thus the system as a whole will be destroyed.

[0010]

Accordingly, the present invention has an object to overcome the above-mentioned drawbacks of the prior art by providing a data recording/playback system, data recording/playback device and method, and data recording medium, adapted to safely keep a content key.

[0011]

The present invention has another object to provide a data recording/playback

system, data recording/playback device and method, and data recording medium, adapted not to leak data to any illegal or unlicensed recorder or to supply data to only a legal or licensed recorder.

[0012]

The present invention has a still another object to provide a data recording/playback system, data recording/playback device and method, and data recording medium, adapted to prevent, if the secret of a legal recorder has been revealed or exposed to outside, new data from being supplied to that recorder.

[0013]

The present invention has a yet another object to provide a data recording/playback system, data recording/playback device and method, and data recording medium, adapted to prevent copyrighted data such as movie, music, etc. from being copied illegally (against the wish of the copyrighter of the data).

[0014]

[Means to Solve the Problem]

According to the present invention, the data recording medium is provided with a security module. Data to be recorded in the data recording medium is encrypted with a content key different from one data to another, and the content key is stored safely in the security module. The security module makes a mutual authentication with a recorder/player (will also be referred to as "unit" hereinafter where appropriate) by the use of a public-key encryption technology, and checks whether its counterpart (the

recorder/player in this case) is a licensed unit before giving the content key to the counterpart. Thus, the security module will not leak the data to any illegal or unlicensed counterpart, namely, to other than the licensed unit. Further, if the secret of a legal unit has been revealed through an attack to the unit, a revocation list issued from a trustable center is effectively used to prevent new data from being given to that legal unit.

[0015]

The above object can be attained by providing a data recording/playback system comprising a data recording medium including a security module, and a data recording/playback device for recording data encrypted with a content key controlled by the security module on the recording medium or playing back the data encrypted with the content key controlled by the security module from the recording medium, wherein the data recording/playback device and the security module execute a mutual authentication protocol using the public-key encryption technology at the time of recording or playing back data.

[0016]

Also the above object can be attained by providing a data recording medium comprising a security module for executing a mutual authentication protocol using a public-key encryption technology with a data recording/playback device at the time of recording and playing back data.

[0017]

Also the above object can be attained by providing a data recording/playback apparatus comprising a control means for executing a mutual authentication protocol using a public-key encryption technology with a security module of a data recording medium at the time of recording and playing back data.

[0018]

Also the above object can be attained by providing a data recording/playback method for recording or playing back data on or from a data recording medium by a data recording/playback device, comprising the step wherein a security module included in the data recording medium and the data recording/playback device execute a mutual authentication protocol using the public-key encryption technology.

[0019]

Also the above object can be attained by providing a data recording medium comprising a security module having an interface function for interfacing with an external unit, a random number generating function, a data storing function, and a calculating function to provide a necessary calculation for mutual authentication protocol using the public-key encryption technology.

[0020]

[Preferred Embodiment of the Invention]

Preferred embodiment of the present invention will now be described with reference to the drawings.

[0021]

Referring now to FIG. 1, there is illustrated an example construction of an optical disc as an example of the data recording medium according to an embodiment of the present invention. The optical disc as the data recording medium will be referred to as "optical disc medium" hereinafter.

[0022]

As shown, the optical disc medium10 includes a cartridge 11 in which an optical disc 12 to which data is recorded, and a security module 13. FIG. 2 shows an example construction of the security module 13.

[0023]

As shown in FIG. 2, the security module 13 includes, in addition to the nonvolatile memory 34, an interface unit 31 of a contact or non-contact type for data transfer to and from units outside the security module 13, an arithmetic unit 32, a random number generator 33 to produce a pseudo random number and a controller 35 to control these components.

[0024]

Referring now to FIG. 3, there is schematically illustrated an optical disc recorder/player 100 as an embodiment of the present invention.

[0025]

The optical disc recorder/player 100 is adapted to write or read data to or from the optical disc medium 10. As shown, it includes a spindle motor 101 to spin the optical disc 12 inside the cartridge 11, optical head 102, servo circuit 103,

recording/playback circuit 104, controller to control these components, an input unit 106 connected to the controller 105, random number generator 107, and an interface unit 108.

[0026]

The spindle motor 101 is driven under the control of the servo circuit 103 to spin the optical disc 12. The optical head 102 illuminates the recording surface of the optical disc 12 with a laser beam to write or read data to or from the optical disc 12. The servo circuit 103 drives the spindle motor 101 to spin the optical disc 12 at a predetermined speed (for example, constant linear velocity). Further, the servo circuit 103 controls tracking and focusing of the optical head 102 and also provides a sled servo control.

[0027]

The recording/playback circuit 104 includes an encryption unit 104A and decryption unit 104B, whose mode of operation is switched from one to another by the controller 105. More specifically, when the encryption unit 104A is supplied with an external recording signal, it will encrypt the recording signal and supply the encrypted signal to the optical head 102 which will write it to the optical disc 12. When in the reading mode, the decryption unit 104B decrypts data read by the optical head 102 from the optical disc 12 and delivers the data as a read signal to outside.

[0028]

The input unit 106 is a button, switch, remote controller or the like. When the

user makes an input operation with the input unit 106, the latter will provides a signal corresponding to the user's input operation. The controller 105 controls the entire system according to a stored predetermined program. The random number generator 107 is controlled by the controller 105 to generate a specified random number. The interface unit 108 is of a contact or non-contact type to transfer data to and from the security module 13 in the optical disc medium 10.

[0029]

As shown, the optical disc recorder/player 100 according to an embodiment of the present invention further includes an arithmetic unit 109 and nonvolatile memory 110.

[0030]

In this embodiment of the present invention, each of the security module 13 in the optical disc medium 10 and the optical disc recorder/player 100 is given an identification code (ID) for each medium, private key and public key of a public-key encryption system, corresponding to the ID, and a public key certificate from a trusted center (TC). The security module 13 and the optical disc recorder/player 100 have these data stored in the storage area of the nonvolatile memories 34 and 110, respectively. Especially, the private key is safely stored so that it will not leak to outside.

[0031]

The public key certificate is data including the ID and public key and digitally

signed by the TC.

[0032]

Note that the digital signature technology allows to certify that a certain data has been prepared by a certain user. For example, the so-called "Elliptic Curve Digital Signature Algorithm (EC-DSA)" used in the Institute of Electrical and Electronics Engineers (IEEE) P1363 is well known as one of this technology.

[0033]

According to this embodiment, the nonvolatile memory 34 of the optical disc medium 10 and nonvolatile memory 110 of the optical disc recorder/player 100 have stored therein a common public key of the TC to the whole system to check the digital signature made by the TC, included in the public key certificate.

[0034]

Further, according to this embodiment, each of the nonvolatile memory 34 of the security module 13 of the optical disc medium 10 and nonvolatile memory 110 of the optical disc recorder/player 100 has an area for storage of the revocation list shown in FIG. 4.

[0035]

The revocation list contains a version number being a number increasing monotonously, a list of IDs of optical disc media or optical disc recorder/player units whose private keys have been revealed, and the digital signature made by the TC.

[0036]

If the nonvolatile memory 34 of the security module 13 of the optical disc medium 10 has a small capacity not to be able to store the revocation lists, the revocation lists may be stored in a part of the optical disc 12, not in the nonvolatile memory 34.

[0037]

Also, when the optical disc recorder/player 100 is shipped from factory, it is desirable that the latest revocation list is stored in the nonvolatile memory 110.

[0038]

Next, the procedure for data recording to the optical disc medium 10 by the optical disc recorder/player 100 according to this embodiment will be described below with reference to FIG. 5.

[0039]

The optical disc recorder/player 100 and the security module 13 of the optical disc recording medium 10 respectively have the ID given by the TC, private key and public key of the public-key encryption system, public key certificate and the revocation list.

[0040]

First the optical disc recorder/player 100 sends, to the security module 13 of the optical disc medium 10, a recording command indicating that data is going to be recorded, and a Recording-ID assigned at each recording to identify each recording (step R1).

[0041]

Next, the optical disc recorder/player 100 and the security module 13 of the optical disc medium 10 execute, by the use of the recording command as a trigger, mutual authentication and key sharing protocols using the public-key encryption technology (step R2).

[0042]

The mutual authentication protocol using the public-key encryption technology is to check mutually with a counterpart that the counterpart has a pair (approved by the TC) of the valid public key and private key. It can be prepared using the EC-DSA (Elliptic Curve Digital Signature Algorithm) under standardization by IEEE P1363 for example.

[0043]

It should be noted that in the mutual authentication protocol using the public-key encryption technology, both the security module 13 of the optical disc medium 10 and optical disc recorder/player 100 have to generate a random number by means of their respective functions of random number generation, read their own private keys and public key certificates stored in the their own nonvolatile memories, and execute arithmetic operations based on the public-key encryption technology by means of their own operational functions.

[0044]

In addition to the mutual authentication protocol using the public-key encryption

technology, there has also been known a mutual authentication protocol using the common-key encryption technology. The latter technology is based on an assumption that each of two parties going to execute the protocol has a common key. Since to adopt the mutual authentication protocol using the common-key encryption technology, there should be an inter-operability between the recording medium and recorder/player, all the security module 13 and optical disc recorder/player 100 should have a common key to the whole system. In this case, however, if one of the security modules or optical disc recorder/player units is attacked and has the key thereof revealed, the whole system will be influenced by the revelation.

[0045]

On the contrary, in the mutual authentication protocol using the public-key encryption technology, the recorder/player units and security modules have unique keys, respectively, and the aforementioned revocation list can be used in this embodiment. Therefore, even if the key of one of the recorder/player units is revealed, only the recorder/player having the key thereof revealed can be revoked from the system, whereby the influence on the system can be minimized.

[0046]

The key sharing protocol using the public-key encryption technology is to safely share secret data between two parties, and can be prepared using the so-called Elliptic Curve Diffie Hellman (EC-DH) under standardization by IEEE P1363.

[0047]

As an example of the mutual authentication protocol and key sharing protocol using the public-key encryption technology, there is available the Full Authentication and Key Exchange (FAKE) protocol specified in the so-called Digital Transmission Content Protection (DTCP) standard (this standard itself is not opened to any unlicensed person but the white paper outlining the standard is acquired from a Web page, http://www.dtcp.com of the Digital Transmission Licensing Administrator (DTLA) which is a licensing organization) developed by five companies; Sony, Matsushita, Hitachi, Toshiba and Intel. This FAKE protocol is generally composed of the following steps S1 to S4:

[0048]

(S1) One of the security module and optical disc recorder/player generates a random number by its random number generator, and sends it along with its own public key certificate to the other.

(S2) The one makes calculation based on the public-key encryption technology to check if the other's public key certificate is valid.

(S3) The one makes a calculation (first step) based on the public-key encryption technology for key sharing, and sends the data (result of operation) along with its own digital signature prepared by making calculation based on the public-key encryption technology to the other.

(S4) The one makes calculation based on the public-key encryption technology, as to the data obtained at step S3 and sent from the other, to check the other's digital

signature, and makes calculation (second step) based on the public-key encryption technology for key sharing to calculate the value of the shared key.

[0049]

In this protocol, the one checks, for the mutual authentication, that the other has a correct private key and public key and the other's ID is not listed in its own revocation list (black list). That is, in case a key of a unit, which was valid when the unit was shipped, has been attacked by a so-called reverse engineering or the like and the ID of the unit whose key has thus been revealed is listed in the revocation list, no data will be passed to any unit (to which no data should be passed) listed in the revocation list.

[0050]

Further, the recorder/player and security module of the recording module exchange the version numbers of their own revocation lists between them.

[0051]

When the one has a newer version of the revocation list than that of the revocation list the other owns, it will send its own revocation list to the other. On the other hand, one of the recorder/player and security module of the recording medium, which has the revocation list of a old version, requests the other to send the revocation list of the new version, checks that the revocation list is valid, and then updates its own revocation list to the new version of the revocation list received from the other.

[0052]

It should be noted that the transfer of the revocation list may be done after the data recording described later.

[0053]

As the result of the above-mentioned mutual authentication protocol and key sharing protocol using the public-key encryption technology, the optical disc recorder/player 100 and security module 13 will safely share a key.

[0054]

This shared key will be referred to as "session key (Kse)" hereinafter.

[0055]

Next, a content key (Kc) to encrypt data is determined by using one of the following methods (1) to (4):

[0056]

(1) It is assumed that Kc = Kse. At this time, the security module 13 safely stores the content key Kc into the nonvolatile memory 34 provided therein, or it sends to the optical disc recorder/player 100 a value Enc(Kst, Kc) derived from encryption of the content key Kc with a storage key (Kst) stored in advance therein and records it to the optical disc 12.

(2) It is assumed that the storage key Kst stored in advance in the security module 13 is the content key Kc. In this case, the security module 13 encrypts the storage key Kst with the session key Kse, sends it to the optical disc recorder/player 100.

(3) The security module 13 generates a new content key Kc by means of the random

number generator or the like. In this case, the security module 13 encrypts the content key Kc with the session key Kse and sends it to the optical disc recorder/player 100. The security module 13 safely stores the content key Kc into the nonvolatile memory 34 provided therein, or it sends to the optical disc recorder/player 100 a value Enc(Kst, Kc) derived from encryption of the content key Kc with a storage key (Kst) stored in advance therein and records it to the optical disc 12.

(4) The optical disc recorder/player 100 generates a new content key Kc by means of the random number generator or the like. In this case, the optical disc recorder/player 100 encrypts the content key Kc with the session key Kse, and sends it to the security module 13. The security module 13 safely stores the content key Kc into the nonvolatile memory 34 provided therein, or it sends to the optical disc recorder/player 100 a value Enc(Kst, Kc) derived from encryption of the content key Kc with a storage key (Kst) stored in advance therein and records it to the optical disc 12.

[0057]

When a content key Kc is determined using any one of the above methods (1) to (4), the optical disc recorder/player 100 encrypts, with the content key Kc, data to be recorded into the optical disc 12, and then record the encrypted data Enc (Kc, data) to the optical disc 12 (step R3).

[0058]

Also, when the content key Kc or encrypted content key Kc is recorded into the

nonvolatile memory 34 of the security module 13 or the optical disc 12, it is recorded along with a recording ID (Recording-ID) which is to be a search key or the encrypted content key Kc is recorded in one sector in the optical disc 12 to which the data is to be written so that a correspondence can be established between the data and content key Kc. Note that for management and transfer of the content key Kc and data encryption, a common key encryption algorithm should preferably be used from the standpoint of the processing speed.

[0059]

The common key encryption algorithm is an encryption algorithm using the same content key in both encryption and decryption. As an example of this algorithm, the so-called Data Encryption Standard (DES) designated as one of the United States Standards in FIPS46-2 is available.

[0060]

Among others, by the method (4), the optical disc recorder/player 100 can encrypt data in advance since the method allows the optical disc recorder/player 100 to determine a content key Kc.

[0061]

Data is recorded to the optical disc 12 by following the above procedure.

[0062]

Next, the procedure for reading data from the optical disc 12 by the optical disc recorder/player 100 will be described below with reference to FIG. 6.

[0063]

The optical disc recorder/player 100 and the security module 13 in the optical disc medium 10 respectively have an ID given from the TC, private key and public key of the public-key encryption system, public key certificate and a revocation list.

[0064]

Also, it is assumed that the optical disc recorder/player 100 already knows a recording ID (Recording-ID) appended to data to be read.

[0065]

First the optical disc recorder/player 100 sends a playback command indicating that data is going to be read and the recording ID to the security module 13 (step P1).

[0066]

The optical disc recorder/player 100 and security module 13 execute, by the use of the playback command as a trigger, mutual authentication and key sharing protocols using the public-key encryption technology (step P2).

[0067]

The key sharing protocol is similar to the protocol used in data recording, and allows the security module 13 and optical disc recorder/player 100 to mutually check that their counterparts have correct public key and private key and the IDs of their counterparts are included in the revocation lists their counterparts have respectively, share a session key Kse and to send the version numbers of their own revocation lists to their counterparts. When one of the security module 13 and optical disc

recorder/player 100 has a revocation list whose version number is newer than that of the revocation list the other owns, the one sends the revocation list to the other and the other updates its own revocation list with the received revocation, as in the recording procedure having previously been described. Also, the transfer of the revocation list may be done after the data readout described later.

[0068]

Next, the optical disc recorder/player 100 has to know a content key Kc with which data has been encrypted before reading the data from the optical disc 12.

[0069]

The content key Kc is safely stored in the nonvolatile memory 34 of the security module 13 or recorded in the optical disc 12 as a value Enc(Kst, Kc) obtained by encrypting the content key Kc with a storage key Kst pre-stored in the security module 13.

[0070]

In the former case, the security module 13 sends to the optical disc recorder/player 100 a value obtained by encrypting, with a session key Kse, the content key Kc stored in the nonvolatile memory 34. The optical disc recorder/player 100 obtains the content key Kc by decrypting the value with the session key Kse.

[0071]

On the other hand, in the latter case, first the optical disc recorder/player 100 reads from the optical disc 12 the value Enc(Kst, Kc), and sends it to the security

module 13. The security module 13 obtains the content key Kc by decrypting the value Enc(Kst, Kc) with the storage key Kst and encrypts the value Enc(Kse, Kc) encrypted with the session key Kse, and sends it to the optical disc recorder/player 100 at step P5. The optical disc recorder/player 100 obtains the content key Kc by decrypting the value Enc(Kse, Kc) with the session key Kse.

[0072]

As in the above, the optical disc recorder/player 100 can obtain the content key Kc with which the data has been encrypted.

[0073]

The optical disc recorder/player 100 reads from the optical disc 12 data Enc(Kc, data) encrypted with the content key Kc, and decrypts the data with the content key Kc already obtained to use the data (step P3).

[0074]

The above is the procedure for reading data from the optical disc 12.

[0075]

Next, another embodiment of the present invention will be described herebelow:

[0076]

Referring now to FIG. 7, there is illustrated an example construction of a memory data recording medium 20 according to this embodiment. The memory data recording medium will be referred to as "memory medium" hereunder.

[0077]

As shown, the nonvolatile memory medium 20 is provided, in a cartridge 21, with a nonvolatile memory 22 being a nonvolatile memory whose content can be electrically erased for data recording such as flash ROM or EEPROM, and a security module 23.

[0078]

As shown in FIG. 8, the security module 23 includes an external interface unit 41, arithmetic unit 42, random number generator 43, nonvolatile memory 44, controller 45 and a recording medium interface 46.

[0079]

Namely, the above security module 23 has similar construction and function to those of the security module 13 shown in FIG. 2, and in addition the external interface 41 providing an external interface.

[0080]

Also, the security module 23 has also the recording medium interface (for example, flash ROM interface or the like) 46 for interface with the nonvolatile memory 22 in the cartridge 21. Thus, data recording (write) to, and playback (read) from, the nonvolatile memory 22 are effected through the security module 23.

[0081]

The nonvolatile memory 44 in the security module 23 is used to store important data such as confidential data, data to be protected against falsification, etc. If the capacity of the memory 44 is not sufficient for the purpose, such important data can

be recorded to the large-capacity nonvolatile memory 22 provided outside the security module 23 and destined to record general data. In this case, the confidential data is protected by encrypting it with a storage key safely stored in the nonvolatile memory 44 in the security module 23, while the data to be protected against falsification is protected by calculating a so-called integrity check value (ICV) for a block in the nonvolatile memory 22 which records the important data and storing it in the nonvolatile memory 44 in the security module 23, recalculating the ICV for that block when reading the information from the nonvolatile memory 22 outside the security module 23 and comparing it with the stored one, and thus checking that the data is not falsified.

[0082]

The ICV is a value calculated using a predetermined algorithm taking as input a data and a certain secret value (in this case, storage key of the security module 23) in order to assure the integrity of the data (the data is not falsified). With this measure, only one who knows the secret value can calculate an ICV for a data. So, if the data is changed for example, an ICV calculated by the same method at the time of reading the data will be different from an ICV having been calculated at the time of writing the data and stored in the security module 23, and has a similar function and the security module 23 will be able to know the fact that the data has been changed.

[0083]

For calculation of the ICV, there are available a digital signature algorithm using

the public-key encryption technology, message authentication code (MAC) generation algorithm using the shared key encryption technology, and an algorithm using the locked hash function.

[0084]

For the details, the ICV is referred to, for example, Menezes "Handbook of Applied Cryptography", CRC, ISBN 0-8493-8523-7, pp. 352-368.

[0085]

FIG. 9 shows an example construction of the memory data recorder/player 200 of the nonvolatile memory medium 20 according to this embodiment of the present invention. As shown in FIG. 9, the memory data recorder/player (will be referred to as "memory recorder/player" hereunder) 200 includes an input/output terminal 201, controller 205, input unit 206, random number generator 207, interface unit 208, arithmetic unit 209, nonvolatile memory 210. etc.

The recorder/player 200 is generally similar to the optical disc recorder/player 100 shown in FIG. 3 except that the spindle moor 101, optical head 102, servo circuit 103, etc. for the optical disc 12 are not provided as shown in FIG. 3 and there is provided instead an interface 208 for access to the security module 23, which also functions as an interface for writing/reading data to/from the nonvolatile memory medium 20 via the security module 23. The nonvolatile memory medium 20 is electrically connected to the recorder/player 200 via the input/output terminals 24 and 201.

[0086]

Next, the procedure for data recording to the nonvolatile memory medium 20 by the recorder/player 200 will be described below with reference to FIG. 10.

[0087]

Similarly to the example in FIG. 5, the recorder/player 200 and the security module 23 of the nonvolatile memory medium 20 respectively have the ID given by the TC, private key and public key of the public-key encryption system, public key certificate and the revocation list.

[0088]

First the recorder/player 200 sends, to the security module 23, a recording command indicating that data is going to be recorded, and a Recording-ID assigned at each recording to identify each recording (step R11).

[0089]

Next, the recorder/player 200 and the security module 23 of the nonvolatile memory medium 20 execute, by the use of the recording command as a trigger, mutual authentication and key sharing protocols using the public-key encryption technology (step R12). These protocols are similar to those used in the optical disc recorder/player 100 and allow the security module 23 and recorder/player 200 to mutually check that their counterparts have correct public key and private key and the IDs of their counterparts are included in the revocation lists their counterparts have respectively, share a session key Kse and to send the version numbers of their own revocation lists

to their counterparts. When one of the security module 23 and recorder/player 200 has a revocation list whose version number is newer than that of the revocation list the other owns, the one sends the revocation list to the other and the other updates its own revocation list with the received revocation, as in the recording procedure having previously been described. Also, the transfer of the revocation list may be done after the data readout described later.

[0090]

Also in the second embodiment, a content key Kc for encryption of data is determined as in the first embodiment, but the second embodiment uses one of the following methods (11) to (14):

[0091]

(1) It is assumed that Kc = Kse. Namely, a session key Kse obtained with the mutual authentication protocol and key sharing protocol is taken as a content key Kc. At this time, the security module 23 safely stores the content key Kc into the nonvolatile memory 44 provided therein, or it stores into the nonvolatile memory 22 outside the security module 23 a value Enc(Kst, Kc) obtained by encrypting the content key Kc with a storage key (Kst) stored in advance therein.

(12) It is assumed that the storage key Kst stored in advance in the security module 23 is the content key Kc. In this case, the security module 23 encrypts the storage key Kst with the session key Kse, sends it to the recorder/player 200.

(13) The security module 23 generates a new content key Kc by means of the random

number generator or the like. In this case, the security module 23 encrypts the content key Kc with the session key Kse and sends it to the recorder/player 200. Also, the security module 23 safely stores the content key Kc into the nonvolatile memory 44 provided therein, or it stores into the nonvolatile memory 22 a value Enc(Kst, Kc) obtained by encrypting the content key Kc with a storage key (Kst) stored in advance therein.

(14) The recorder/player 200 generates a new content key Kc by means of the random number generator or the like, encrypts data with the content key Kc, and records it. In this case, the recorder/player 200 encrypts the content key Kc with the session key Kse, and sends it to the security module 23. The security module 23 safely stores the content key Kc into the nonvolatile memory 44 provided therein, or it stores into the nonvolatile memory 22 a value Enc(Kst, Kc) derived from encryption of the content key Kc with a storage key (Kst) stored in advance therein.

[0092]

When a content key Kc is determined using any one of the above methods (11) to (14), the recorder/player 200 encrypts, with the content key Kc, data to be recorded into the nonvolatile memory medium 20, and sends the encrypted data Enc (Kc, data) to the security module 23 (step R13).

[0093]

At this time, the security module 23 stores the encrypted data Enc(Kc, data) into the nonvolatile memory 22.

[0094]

Also, when the content key Kc or encrypted content key Kc is recorded into the nonvolatile memory 44 of the security module 23 or nonvolatile memory 22, it is recorded along with a recording ID (Recording-ID) which is to be a search key or the encrypted content key Kc is recorded in the same sector as in the nonvolatile memory 22 in which the data is to be recorded so that a correspondence can be established between the data and content key Kc.

[0095]

Among others, by the method (14), the recorder/player 200 can encrypt data in advance since the method allows the recorder/player 200 to determine a content key Kc.

[0096]

Data is recorded to the nonvolatile memory medium 20 by following the above procedure.

[0097]

Meanwhile, data recording may be effected as shown in FIG. 11.

[0098]

The recorder/player 200 encrypts data with a session key Kse shared by itself and security module 23 by the mutual authentication and key sharing protocols, and send the encrypted data to the security module 23 (step R2).

[0099]

The security module 23 decrypts the data with the session key Kse to obtain data in plaintext, and records a value Enc(Kc, data) encrypted with a newly generated content key Kc into the data memory 22 (step R24).

[0100]

The security module 23 stores the content key Kc safely into the internal nonvolatile memory 44 or stores into the nonvolatile memory 22 a value Enc(Kse, Kc) obtained by encrypting the content key Kc with a storage key Kst previously stored in the security module 23. Thus, the security module 23 will not have to teach even the recorder/player 200 the content key Kc for the data.

[0101]

Data is recorded to the memory medium by following the above procedure.

[0102]

Next, the procedure for reading data from the nonvolatile memory medium 20 by the recorder/player 200 will be described below with reference to FIG. 12.

[0103]

The recorder/player 200 and the security module 23 in the nonvolatile memory medium 20respectively have an ID given from the TC, private key and public key of the public-key encryption system, public key certificate and a revocation list. Also, it is assumed that the recorder/player 200 already knows a recording ID appended to data to be read.

[0104]

First the recorder/player 200 sends a playback command indicating that data is going to be read and the recording ID to the security module 23 (step P11).

[0105]

Next the recorder/player 200 and security module 23 of the nonvolatile memory medium 20 execute, by the use of the playback command as a trigger, mutual authentication and key sharing protocols using the public-key encryption technology (step P12).

[0106]

The protocols are similar to those used in the data recording, and allow the security module 23 and recorder/player 200 to mutually check that their counterparts have correct public key and private key and the IDs of their counterparts are included in the revocation lists their counterparts have respectively, share a session key Kse and to send the version numbers of their own revocation lists to their counterparts. When one of the security module 23 and recorder/player 200 has a revocation list whose version number is newer than that of the revocation list the other owns, the one sends the revocation list to the other and the other updates its own revocation list with the received revocation. It should be noted that the transfer of the revocation list may be done after the data recording.

[0107]

Next, the recorder/player 200 has to know a content key Kc with which data has been encrypted before reading the data from the nonvolatile memory 22 of the

nonvolatile memory medium 20.

[0108]

The content key Kc is safely stored in the nonvolatile memory 44 of the security module 23 or recorded in the nonvolatile memory 22 as a value Enc(Kst, Kc) obtained by encrypting the content key Kc with a storage key Kst pre-stored in the security module 23.

[0109]

In the former case, the security module 23 sends to the recorder/player 200 a value obtained by encrypting, with a session key Kse, the content key Kc stored in the nonvolatile memory 44. The recorder/player 200 obtains the content key Kc by decrypting the value with the session key Kse.

[0110]

On the other hand, in the latter case, first the security module 23 reads from the nonvolatile memory 22 the value Enc(Kst, Kc), and decrypts the value Enc(Kst, Kc) with the storage key Kst to provide the content key Kc. Further, the security module 23 obtains the value Enc(Kse, Kc) obtained by encrypting the content key Kc the session key Kse, and sends it to the recorder/player 200. The recorder/player 200 obtains the content key Kc by decrypting the value Enc(Kse, Kc) with the session key Kse.

[0111]

As in the above, the recorder/player 200 can obtain the content key Kc with

which the data has been encrypted.

[0112]

Thereafter, the recorder/player 200 reads, from the nonvolatile memory 22, data Enc(Kc, data) encrypted with the content key Kc via the security module 23 (step P13), and decrypts the data with the content key Kc already obtained to use the data (step P14).

[0113]

The above is the basic procedure for reading data from the memory medium.

[0114]

Meanwhile, a procedure like the data recording procedure shown in FIG. 13 may be used as the data playback procedure in this embodiment.

[0115]

That is, the security module 23 does not send the content key Kc to the recorder/player 200, but reads out the encrypted content data Enc(Kc, data) from the nonvolatile memory 22 (step P23), and decrypts, with the content key Kc, the encrypted content data Enc(Kc, data) to obtain a plaintext, and encrypts the decrypted data using the session key Kse shared as a result of an authentication and key sharing protocol to send the encrypted content data Enc(Ksc, data) to the recorder/player 200 (step P24).

[0116]

The recorder/player 200 decrypts the data Enc(Kse, data) with its own session

Kse, to thereby obtain the plaintext data for use (step P25).

[0117]

Thus, the security module 23 will not have to teach the recorder/player 200 the content key Kc with which the data has been encrypted.

[0118]

Data is read out from the memory medium by following the above procedure.

[0119]

Meanwhile, although an optical disc medium and a nonvolatile memory medium 20 have been exemplified as a data recording medium to which the present invention is applied, the recording medium is not limited to these, but may be a magnetic disc, magnetic tape, magneto-optical disc, or a volatile memory backed up by a battery.

[0120]

[Effect of the Invention]

As having been described in the foregoing, according to the present invention, each of the recording media is provided with a security module, and data to be recorded to the recording medium is encrypted with a content key different from one data to another and the content key can safely be stored in the security module.

[0121]

Also, according to the present invention, the security module makes a mutual authentication using a public-key encryption technology with the recorder/player at the time of data recording or playback, the content key is given to a counterpart after the

counterpart is judged to be a legally licensed unit, thereby allowing to prevent data from being leaked to any illegal unit.

[0122]

Furthermore, according to the present invention, revocation lists issued from the trustable or trusted center can effectively be utilized to prevent data from being given to a unit which is legal but has been attacked and thus has its own secret revealed or exposed to outside.

[0123]

Therefore, according to the present invention, it is possible to prevent copyrighted data such as movie and music from illegally being copied.

[Brief Description of the Drawings]

FIG. 1 shows the construction of an optical disc as the data recording medium according to the present invention.

FIG. 2 is a block diagram of an example of the security module included in the optical disc as the data recording medium.

FIG. 3 is a block diagram of an optical disc recorder/player according to the present invention.

FIG. 4 explains a revocation list.

FIG. 5 shows a basic procedure for writing data to the optical disc as the data recording medium according to the present invention.

FIG. 6 shows a basic procedure for reading data from the optical disc as the data

recording medium according to the present invention.

FIG. 7 shows the construction of a nonvolatile memory medium according to the present invention.

FIG. 8 is a block diagram of an example of the security module included in the nonvolatile memory medium.

FIG. 9 is a block diagram of a nonvolatile memory recorder/player according to the present invention.

FIG. 10 shows a basic procedure for writing data to the nonvolatile memory recorder/player according to the present invention.

FIG. 11 shows another example of the procedure for writing data to the nonvolatile memory recorder/player according to the present invention.

FIG. 12 shows a basic procedure for reading data from the nonvolatile memory recorder/player according to the present invention.

FIG. 13 shows another example of the procedure for reading data from the nonvolatile memory recorder/player according to the present invention.

[Explanation of Referenced Numerals]

10 optical disc medium; 11 cartridge; 12 optical disc; 13 security module; 31 interface unit; 32 arithmetic unit; 33 random number generator; 34 nonvolatile memory; 35 controller; 100 optical disc recorder/player; 101 spindle motor; 102 optical head; 103 servo circuit; 104 recording/playback circuit; 105 controller; 106 input unit; 107 random number generator; 108 interface unit; 109 arithmetic unit; 110 nonvolatile

memory; 20 nonvolatile memory medium; 21 cartridge; 22 nonvolatile memory; 23 security module; 24 input/output terminal; 41 external interface; 42 arithmetic unit; 43 random number generator; 45 controller; 46 recording medium interface; 200 memory recorder/player; 201 input/output terminal; 205 controller; 206 input unit; 207 random number generator; 208 interface unit; 209 arithmetic unit; 210 nonvolatile memory